

4.2.4 Anti-malware Software

Syllabus 2026 - 2028

WHAT YOU NEED TO KNOW

- The use of anti-malware and anti-virus software
- The operation of removing or quarantining viruses using up-to-date software
- Scanning the storage media used to transfer data
- Scanning data and software when downloading

Malware and anti-malware

Malware is malicious software designed to harm a computer or steal data. Examples are viruses, worms, trojans, spyware, ransomware and adware. **Anti-virus** software finds and removes viruses, and **anti-malware** software protects against the wider range of malicious software, including spyware. Most products now do both.

How it works

- **Scanning:** checks files, programs and memory, either at set times or when a file is opened, copied or downloaded (real-time protection)
- **Signature checking:** compares files with a database of known malware, called virus definitions
- **Behaviour checking (heuristics):** looks for suspicious behaviour, to find new malware that is not yet in the database
- **Quarantine:** isolates a suspicious file in a safe area so that it cannot run or spread, while keeping it so it can be checked or restored if it was a false alarm
- **Removing:** the infected file is cleaned (the malware is removed) or deleted, and the user is told

Figure 10: How anti-malware software checks a file



Why it must be up to date

New malware appears every day. Anti-malware can only find what it knows about, so the software and its virus definitions must be updated regularly, ideally automatically. Out-of-date software will miss new threats.

Scanning storage media and downloads

- **Storage media used to transfer data:** memory sticks, external drives, discs and memory cards can carry malware from one computer to another. Scan them before opening any file on them
- **Downloads:** scan files, programs and email attachments when they are downloaded and before they are opened or installed
- Only download from trusted sources, and do not open attachments from unknown senders

Advantages	Disadvantages
+ Finds and removes malware automatically	- Can slow down the computer while scanning

Advantages	Disadvantages
+ Protects personal data, files and passwords	- Cannot detect brand-new malware until its definitions are added
+ Real-time protection stops threats before damage is done	- May give false alarms and block safe files
+ Scans can be scheduled so users do not have to remember	- Needs regular updates, which use data and time
+ Prevents malware spreading to other computers	- Good products cost money, and users can be careless by trusting it too much

EXAM TIP

Say **quarantine** means 'isolated so it cannot run', not 'deleted'. A quarantined file can be cleaned, deleted or restored later. And always give the reason for updates: new malware appears all the time.

Key terms

Term	Meaning
Malware	Software designed to harm a computer or steal data.
Virus	Malware that copies itself and spreads, often damaging files.
Spyware	Malware that secretly records a user's activity.
Virus definitions	The database of known malware used for scanning.
Heuristic checking	Detecting malware from suspicious behaviour.
Quarantine	Isolating a suspicious file so it cannot run.
Real-time protection	Scanning files automatically as they are used.
False positive	A safe file wrongly flagged as malware.

Practice questions

Answer each question in full sentences. Command words used: State (give a short answer), Describe (say what it is like), Explain (give reasons), Analyse (break it down and examine it), Suggest (apply your knowledge to a situation), Compare and contrast (similarities and differences), Evaluate (weigh up and reach a judgement).

No.	Question	Marks
1	State two examples of malware.	[2]
2	Describe how anti-malware software finds malware on a computer.	[3]
3	Explain why anti-malware software must be kept up to date.	[2]
4	Analyse why a memory stick should be scanned before its files are opened on a school computer.	[3]
5	Suggest two precautions a user should take when downloading a program from the internet.	[2]
6	Compare and contrast quarantining an infected file with deleting it.	[3]
7	Evaluate the use of anti-malware software to protect a school network.	[5]

Total: 20 marks